UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

CHRISTOPHER ROY, on behalf of himself and all others similarly situated, Plaintiff, v. **HUB INTERNATIONAL LIMITED,** Defendant.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Christopher Roy ("Plaintiff"), individually and on behalf of all similarly situated persons, alleges the following against HUB International Limited ("HUB" or "Defendant") based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by Plaintiff's counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against HUB for its failure to properly secure and safeguard Plaintiff's and over 479,000 similarly situated individuals' names, driver's license numbers, social security numbers, and financial account information (the "Private Information") from hackers.[1]

2. HUB, based in Chicago, Illinois, is an insurance brokerage that serves more than 450,000 customers throughout the United States and internationally.

[1] *See* https://www.mass.gov/doc/data-breach-report-2023/download (last visited Aug. 23, 2023).

3. On or about July 27, 2023, HUB filed official notice of a hacking incident with the office of the Maine Attorney General.

4. On or about August 11, 2023, HUB also sent out data breach notice letters (the "Notice") to individuals whose information was compromised as a result of the hacking incident.

5. Based on information provided in the Notice sent to impacted individuals, HUB detected unusual activity on some of its computer systems in or around January 17, 2023. In response, the company isolated the impacted systems and launched an investigation which revealed that an unauthorized party had access to certain company files between December 12, 2022, and January 17, 2023 (the "Data Breach"). Yet, HUB waited over six months to notify the public that they were at risk.

6. As a result of this delayed response, Plaintiff and "Class Members" (defined below) had no idea for over *six months* that their Private Information had been impacted, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. This risk will remain for their respective lifetimes.

7. The Private Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves, including but not limited to, driver's license number, social security number, and financial account information that HUB collected and maintained.

8. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax

returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

9. There has been no assurance offered by HUB that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

10. Therefore, Plaintiff and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

11. Plaintiff brings this class action lawsuit to address HUB's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and its failure to provide timely and adequate notice to Plaintiff and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

12. The potential for improper disclosure and theft of Plaintiff's and Class Members' Private Information was a known risk to HUB, and thus HUB was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

13. Upon information and belief, HUB failed to properly monitor and implement security practices regarding the computer network and systems that housed the Private Information. Had HUB properly monitored its networks, it would have discovered the Breach sooner.

14. Plaintiff's and Class Members' identities are now at risk because of HUB's negligent conduct as the Private Information that HUB collected and maintained is now in the hands of data thieves and other unauthorized third parties.

15. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed and compromised during the Data Breach.

16. Accordingly, Plaintiff, on behalf of himself and the Class, asserts claims for Negligence, Negligence *Per Se*, Breach of Third-Party Beneficiary Contract, Invasion of Privacy, Unjust Enrichment, and Violations of the Illinois Consumer Fraud and Deceptive Business Practices Act.

II. PARTIES

17. Plaintiff Christopher Roy, is, and at all times mentioned herein was, an individual citizen of the State of Massachusetts.

18. Defendant HUB is an insurance brokerage incorporated in Illinois with its principal place of business at 150 N. Riverside Plaza 17th Floor, Chicago, Illinois, 60606 in Cook County.

III. JURISDICTION AND VENUE

19. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from HUB. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

20. This Court has jurisdiction over HUB because HUB operates in and is incorporated in this District.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and HUB has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. HUB's Business and Collection of Plaintiff's and Class Members' Private Information

22. HUB is a global insurance brokerage. Founded in 1998, HUB provides its customers with insurance-based wealth management, serving more than 450,000 customers in Illinois and across the country. HUB employs more than 16,000 people in North America and is valued at approximately $23 billion, generating $4 billion in annual revenue.

23. As a condition of receiving financial services, HUB requires that its customers entrust it with highly sensitive personal information belonging to employees and other individuals, like Plaintiff and Class Members. In the ordinary course of receiving service from HUB, Class Members were required to provide their Private Information to Defendant.

24. HUB uses this information, *inter alia*, for business and affiliate marketing purposes.

25. In its privacy policy, HUB promises that it maintains "technical and organizational security measures reasonably designed to protect the security of your Personal Information against loss, misuse, unauthorized access, disclosure, or alteration."[2] HUB also claims that it "take[s] very seriously our privacy responsibilities to you, and we are committed to treating your Personal Information in a manner that is consistent with applicable law and this Policy."[3]

26. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, HUB assumed legal and equitable duties and knew or should have

[2] *See* https://www.hubinternational.com/about-us/privacy-policy/ (last visited on Aug. 23, 2023).
[3] *Id.*

known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

B. The Data Breach and HUB's Inadequate Notice to Plaintiff and Class Members

27. On or about August 11, 2023, roughly *six months* after HUB learned that the Class's Private Information was first accessed by cybercriminals, HUB finally began to notify individuals that its investigation determined that their Private Information was impacted.

28. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including social security numbers, driver's license numbers, and financial account information.

29. The Notice sent to Plaintiff and Class Members attached pages entitled "Steps You Can Take to Protect Personal Information," which listed generic and time-consuming steps that victims of data security incidents should take to mitigate the devastating impacts of data breaches like the HUB Data Breach, such as getting a copy of a credit report or notifying law enforcement about suspicious financial account activity.

30. Other than providing only two years of credit monitoring that Plaintiff and Class Members would have to affirmatively sign up for, HUB offered no other substantive steps to help victims like Plaintiff and Class Members to protect themselves. On information and belief, HUB sent a similar generic Notice to all individuals affected by the Data Breach.

31. HUB had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

32. HUB took possession of Plaintiff's and Class Members' Private Information with the understanding that it would comply with its obligations to keep such Information confidential

and secure from unauthorized access, timely detect any breaches and/or unauthorized disclosures of such Information, and to provide timely notice of any security breaches.

33. HUB's data security obligations were particularly important given the substantial increase in cyberattacks in recent years. HUB knew or should have known that its electronic records would be targeted by cybercriminals.

C. HUB Failed to Comply with FTC Guidelines

34. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

35. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

36. The FTC further recommends that companies not maintain personally identifiable information ("PII") longer than is needed for authorization of a transaction, limit access to sensitive

data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

37. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

38. As evidenced by the Data Breach, HUB failed to properly implement basic data security practices. HUB's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

39. HUB was at all times fully aware of its obligation to protect the Private Information belonging to Plaintiff and Class Members yet failed to comply with such obligations. It was also aware of the significant repercussions that would result from its failure to do so.

D. HUB Failed to Comply with Industry Standards

40. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

41. Some industry best practices that should be implemented by businesses like HUB include but are not limited to educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As

evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

42. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

43. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

44. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

E. HUB Breached its Duty to Safeguard Plaintiff's and Class Members' Private Information

45. In addition to its obligations under federal and state laws, HUB owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. HUB owed a duty to Plaintiff and Class Members to provide reasonable security, including complying with industry

standards and requirements, training for its staff, and ensuring that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

46. HUB breached its obligations to Plaintiff and Class Members and was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. HUB's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect Plaintiff's and Class Members' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of the Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

47. HUB negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

48. Had HUB remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field,

it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

49. Accordingly, Plaintiff's and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Class Members also lost the benefit of the bargain they made with HUB.

F. HUB Should Have Known that Cybercriminals Target Private Information to Carry Out Fraud and Identity Theft

50. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[4] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

51. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

[4] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on Aug. 23, 2023).

52. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

53. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

54. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

55. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a

freeze on their credit, and correcting their credit reports.[5] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

56. Identity thieves can also use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

57. PII is data that can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

58. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[6] The increase in cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendants' industry, including Defendants, who had already experienced a recent breach.

---

[5] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited Aug. 23, 2023).

[6] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice, Feb. 10, 2020, available at https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-fourmembers-china-s-military (last visited on Aug. 23, 2023).

59. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[7] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web and that the "*fullz*" (a term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for $30 in 2017.[8]

60. Furthermore, even information such as names, email addresses and phone numbers, can have value to a hacker. Beyond things like spamming customers, or launching phishing attacks using their names and emails, hackers, *inter alia*, can combine this information with other hacked data to build a more complete picture of an individual. It is often this type of piecing together of a puzzle that allows hackers to successfully carry out phishing attacks or social engineering attacks. This is reflected in recent reports, which warn that "[e]mail addresses are extremely valuable to threat actors who use them as part of their threat campaigns to compromise accounts and send phishing emails."[9]

61. The Dark Web Price Index of 2022, published by PrivacyAffairs[10] shows how valuable just email addresses alone can be, even when not associated with a financial account:

---

[7] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited on Aug. 23, 2023).

[8] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited on Aug. 23, 2023).

[9] *See* https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/ (last visited on Aug. 23, 2023).

[10] *See* https://www.privacyaffairs.com/dark-web-price-index-2022/ (last visited on Aug. 23, 2023).

Email Database Dumps	Avg. Price USD (2022)
10,000,000 USA email addresses	$120
600,000 New Zealand email addresses	$110
2,400,000 million Canada email addresses	$100

62. Beyond using email addresses for hacking, the sale of a batch of illegally obtained email addresses can lead to increased spam emails. If an email address is swamped with spam, that address may become cumbersome or impossible to use, making it less valuable to its owner.

63. Likewise, the value of PII is increasingly evident in our digital economy. Many companies including HUB collect PII for purposes of data analytics and marketing.[11]

64. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[12]

65. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not only by a price at which consumers or hackers actually seek to sell it, but rather by the economic benefit consumers derive from being able to use it and control the use of it.

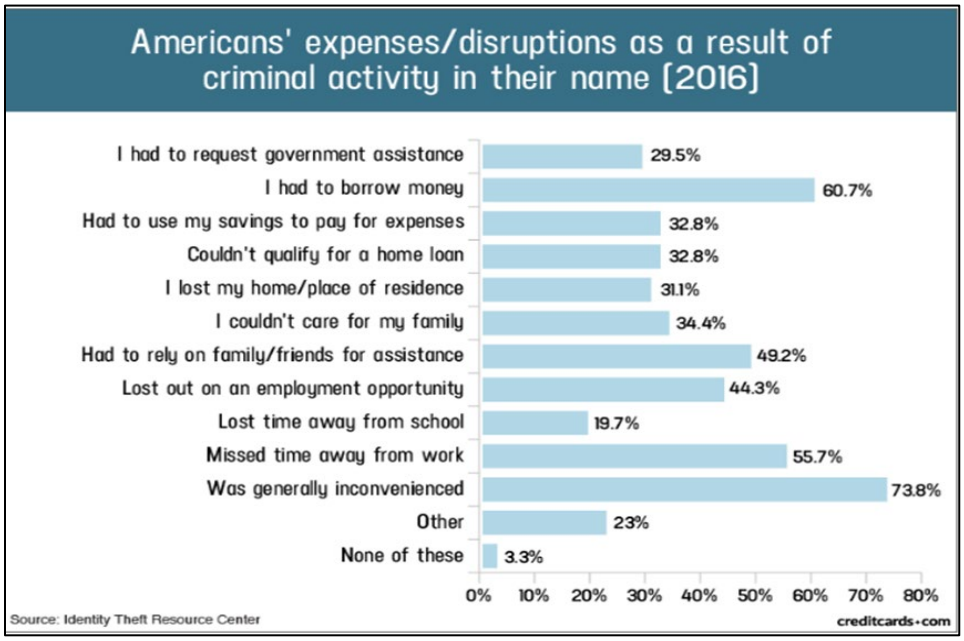
66. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

[11] *See* https://robinhood.com/us/en/support/articles/privacy-policy/ (last visited on Aug. 23, 2023).

[12] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets,* 15 Rich. J. L. & Tech. 11, 14 (2009).

67. Data breaches, like that at issue here, damage consumers by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiff's PII impairs his ability to participate in the economic marketplace.

68. A study by the Identity Theft Resource Center[13] shows the multitude of harms caused by fraudulent use of PII:



69. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[14]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on

[13] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited Aug. 23, 2023).

[14] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited Aug. 23, 2023).

> the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

70. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

71. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

G. Plaintiff's and Class Members' Damages

Plaintiff Christopher Roy's Experience

72. Defendant obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure, though Plaintiff is currently unsure how Defendant came into possession of his Private Information.

73. Plaintiff received the Notice from Defendant on or around August 11, 2023 notifying him that his Private Information had been identified by HUB as being "accessed" and "copied" by an unauthorized actor between December 2022 and January 2023.

74. Defendant deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him of the Breach for months.

75. As a result of the Data Breach, Defendant exposed Plaintiff's Private Information for theft by cybercriminals and sale on the dark web.

76. The notice letter offered Plaintiff only two years of credit monitoring services. Two years of credit monitoring is not sufficient given that Plaintiff will now experience a lifetime of

increased risk of identity theft and other forms of targeted fraudulent misuse of his Private Information.

77. Plaintiff suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and monitoring his accounts for fraud.

78. Plaintiff suffered actual injury in the form of having his Private Information compromised and stolen as a result of the Data Breach.

79. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of his personal information, which was compromised in, and as a result of, the Data Breach.

80. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Private Information being placed in the hands of criminals.

81. Plaintiff has a continuing interest in ensuring that his Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

82. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant, as well as long-term credit monitoring options he will now need to use. Plaintiff has spent several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

83. As a result of the Data Breach, Plaintiff has suffered anxiety as a result of the release of his Private Information to cybercriminals, which Private Information he believed would be protected from unauthorized access and disclosure. These feelings include anxiety about

unauthorized parties viewing, selling, and using his Private Information for purposes of committing cyber and other crimes against him. Plaintiff is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on his life.

84. Plaintiff also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

85. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

86. In sum, Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

87. Plaintiff and Class members trusted that their Private Information would remain private without unauthorized disclosure.

88. Plaintiff and Class Members relied on HUB to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this information, which Defendant ultimately failed to do.

89. According to Defendant's Notice, it learned of unauthorized access to its computer systems on January 17, 2023, with such unauthorized access having taken place between December 12, 2022, and January 17, 2023.

90. Plaintiff's Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

91. As a direct and proximate result of HUB's actions and omissions, Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

92. Further, as a direct and proximate result of HUB's conduct, Plaintiff and Class Members have been forced to spend time dealing with the effects of the Data Breach.

93. Plaintiff and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiff and Class Members.

94. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiff and Class Members.

95. Additionally, as a direct and proximate result of HUB's conduct, Plaintiff and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial

accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

96. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

97. Plaintiff and Class Members also suffered a loss of value of their PII and PHI when it was accessed, viewed, and acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists.[15] In 2019, the data brokering industry was worth roughly $200 billion. In fact, the data marketplace is so sophisticated that consumers can sell their non-public information directly to a data broker who in turn aggregates the information and provides it to other companies.[16] Consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[17]

98. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by

[15] See Data Coup, https://datacoup.com/ (last visited on Aug. 23, 2023).
[16] *What is digi.me?, DIGI.ME,* https://digi.me/what-is-digime/ (last visited on Aug. 23, 2023).

[17] *Frequently Asked Questions,* Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited on Aug. 23, 2023).

Plaintiff and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiff and the Class Members, thereby causing additional loss of value.

99. Finally, Plaintiff and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

100. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of HUB, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

101. As a direct and proximate result of HUB's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

102. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

103. Specifically, Plaintiff proposes the following Nationwide Class, as well as the following Illinois Subclass definitions (also collectively referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
>
> All individuals in the United States who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.
>
> **Illinois Subclass**

> All individuals residing in Illinois who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

104. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

105. Plaintiff reserves the right to modify or amend the definitions of the proposed Nationwide Class and Illinois Subclass before the Court determines whether certification is appropriate.

106. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

107. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of more than 450,000 individuals whose Private Information was compromised in the Data Breach. The identities of Class Members are ascertainable through HUB's records, Class Members' records, publication notice, self-identification, and other means.

108. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether HUB engaged in the conduct alleged herein;

b. When HUB learned of the Data Breach;

c. Whether HUB's response to the Data Breach was adequate;

d. Whether HUB unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

e. Whether HUB failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

f. Whether HUB's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether HUB's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether HUB owed a duty to Class Members to safeguard their Private Information;

i. Whether HUB breached its duty to Class Members to safeguard their Private Information;

j. Whether hackers obtained Class Members' Private Information via the Data Breach;

k. Whether HUB had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

l. Whether HUB breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

m. Whether HUB knew or should have known that its data security systems and monitoring processes were deficient;

n. What damages Plaintiff and Class Members suffered as a result of HUB's misconduct;

o. Whether HUB's conduct was negligent;

p. Whether HUB's conduct was *per se* negligent;

q. Whether HUB was unjustly enriched;

r. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

109. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

110. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

111. Predominance. HUB has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from HUB's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

112. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for HUB. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

113. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). HUB has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

114. Finally, all members of the proposed Class are readily ascertainable. HUB has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by HUB.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of Plaintiff and the Nationwide Class or, Alternatively, the Illinois Subclass)

115. Plaintiff restates and realleges all of the allegations stated above and hereafter as if fully set forth herein.

116. HUB knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

117. HUB's duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

118. HUB knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security. HUB was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

119. HUB owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. HUB's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect Plaintiff's and Class Members' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiff and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

120. HUB's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

121. HUB's duty also arose because Defendant was bound by industry standards to protect Plaintiff's and Class Members' confidential Private Information.

122. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and HUB owed them a duty of care to not subject them to an unreasonable risk of harm.

123. HUB, through its actions and omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within HUB's possession.

124. HUB, by its actions and omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

125. HUB, by its actions and omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

126. HUB breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

127. HUB acted with reckless disregard for the rights of Plaintiff and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiff and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

128. HUB had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust HUB with their Private Information was predicated on the understanding that HUB would take adequate security precautions. Moreover, only HUB had the ability to protect its systems (and the Private Information that it stored on them) from attack.

129. HUB's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised and exfiltrated alleged herein.

130. HUB's breaches of duty also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their Private Information, and loss of time and money to monitor their accounts for fraud.

131. As a result of HUB's negligence in breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

132. HUB also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the Data Breach.

133. As a direct and proximate result of HUB's negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

134. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

135. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

136. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring HUB to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On behalf of Plaintiff and the Nationwide Class or, Alternatively, the Illinois Subclass)

137. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

138. Pursuant to Section 5 of the FTCA, HUB had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiff and Class Members.

139. HUB breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

140. Plaintiff and Class Members are within the class of persons that the FTCA is intended to protect.

141. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of HUB's duty in this regard.

142. HUB violated the FTCA by failing to use reasonable measures to protect the Private Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

143. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Private Information in compliance with applicable laws would result in an

unauthorized third-party gaining access to HUB's networks, databases, and computers that stored Plaintiff's and Class Members' unencrypted Private Information.

144. HUB's violations of the FTCA constitute negligence *per se*.

145. Plaintiff's and Class Members' Private Information constitutes personal property that was stolen due to HUB's negligence, resulting in harm, injury, and damages to Plaintiff and Class Members.

146. As a direct and proximate result of HUB's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

147. HUB breached its duties to Plaintiff and the Class under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

148. As a direct and proximate result of HUB's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

149. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring HUB to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT III
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On behalf of Plaintiff and the Nationwide Class or, Alternatively, the Illinois Subclass)

153. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

154. Upon information and belief, Defendant entered into contracts to provide insurance brokerage services to its clients including, Plaintiff believes, his employer, which services included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was to be entrusted to it.

155. Upon information and belief, these contracts are virtually identical.

156. These contracts were made expressly for the benefit of Plaintiff and the Class, as it was their Private Information that Defendant agreed to receive and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties.

157. HUB knew that if it were to breach these contracts with its clients, the clients' employees, including Plaintiff, would be harmed.

158. HUB breached its contracts with its clients whose employees were affected by this Data Breach when it failed to use reasonable data security measures that could have prevented the Data Breach.

159. As foreseen, Plaintiff and the Class were harmed by HUB's failure to use reasonable data security measures to store highly sensitive personal information, including but not limited to, the continuous and substantial risk of harm through the loss of their Private Information.

160. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with costs and attorneys' fees incurred in this action.

COUNT IV
INTRUSION UPON SECLUSION / INVASION OF PRIVACY
(On behalf of Plaintiff and the Nationwide Class or, Alternatively, the Illinois Subclass)

150. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

151. Plaintiff and Class Members maintain a privacy interest in their Private Information, which is private, confidential information that is also protected from disclosure by applicable laws set forth above.

152. Plaintiff and Class Members' Private Information was contained, stored, and managed electronically in HUB's records, computers, and databases that was intended to be secured from unauthorized access to third-parties because highly sensitive, confidential matters regarding Plaintiff's and Class Members' identities were only shared with HUB for the limited purpose of obtaining and paying for Defendant's services.

153. Additionally, Plaintiff's and Class Members' Private Information is highly attractive to criminals who can nefariously use such Private Information for fraud, identity theft, and other crimes without the victims' knowledge and consent.

154. HUB's disclosure of Plaintiff's and Class Members' Private Information to unauthorized third parties as a result of its failure to adequately secure and safeguard their Private Information is offensive. HUB's disclosure of Plaintiff's and Class Members' Private Information to unauthorized third parties permitted the physical and electronic intrusion into private quarters where Plaintiff's and Class Members' Private Information was stored.

155. Plaintiff and Class Members have been damaged by HUB's conduct, including by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT V
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Nationwide Class or, Alternatively, the Illinois Subclass)

156. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

157. This Count is pleaded in the alternative to Count III above.

158. Plaintiff and Class Members conferred a benefit on HUB when their Private Information was turned over to Defendant.

159. Upon information and belief, HUB funds its data security measures entirely from its general revenue, including from payments made to it by Class Members.

160. As such, a portion of the payments made by Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to HUB.

161. HUB has retained the benefits of its unlawful conduct, including the amounts of payment received from Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

162. HUB knew that Plaintiff and Class Members conferred a benefit upon it, which HUB accepted. HUB profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiff's and Class Members' Private Information and prevented the Data Breach.

163. If Class Members had known that HUB had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

164. Due to HUB's conduct alleged herein, it would be unjust and inequitable under the circumstances for HUB to be permitted to retain the benefit of its wrongful conduct.

165. As a direct and proximate result of HUB's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity to control how their Private Information is used; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in HUB's possession and is subject to further unauthorized disclosures so long as HUB fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

166. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from HUB and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by HUB from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

167. Plaintiff and Class Members may not have an adequate remedy at law against HUB, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VI
Violations of the Illinois Consumer Fraud and Deceptive Business Practices Act ("CFA"), 815 Ill. Comp. Stat. §§ 505/1, *et seq.*

168. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

169. Plaintiff and the Class are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiff, the Class, and Defendant are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

170. Defendant engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendant engages in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

171. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the CFA, including: (i) failing to maintain adequate data security to keep Plaintiff's and the Class Members' sensitive PII from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (ii) failing to disclose or omitting materials facts to Plaintiff and the Class regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the PII of Plaintiff and the Class; (iii) failing to disclose or omitting materials facts to Plaintiff and the Class about Defendant's failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII of Plaintiff and the

Class; and (iv) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff's and the Class's PII and other PII from further unauthorized disclosure, release, data breaches, and theft.

172. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about their inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff and the Class and defeat their reasonable expectations about the security of their PII.

173. Defendant intended that Plaintiff and the Class rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

174. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Class. Plaintiff and the Class have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

175. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiff and the Class of the nature and extent of the Data Breach pursuant to the Illinois PII Protection Act, 815 ILCS 530/1, *et seq*.

176. As a result of Defendant's wrongful conduct, Plaintiff and the Class were injured in that they never would have provided their PII to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII from being hacked and taken and misused by others.

177. As a direct and proximate result of Defendant's violations of the CFA, Plaintiff and the Class have suffered harm: (i) actual identity theft; (ii) the loss of the opportunity how their PII

is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

178. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff and the Class seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the CFA.

COUNT VII
DECLARATORY JUDGMENT
(On behalf of Plaintiff and the Class)

179. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

180. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal statutes described in this Complaint.

181. HUB owes a duty of care to Plaintiff and Class Members, which required it to adequately secure Plaintiff's and Class Members' Private Information.

182. HUB still possesses Private Information regarding Plaintiff and Class Members.

183. Plaintiff alleges that HUB's data security measures remain inadequate. Furthermore, Plaintiff continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

184. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. HUB owes a legal duty to secure the Private Information stored on its systems and within its network, and to timely notify victims of a data breach under the common law and Section 5 of the FTCA;

b. HUB's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect Private Information; and

c. HUB continues to breach this legal duty by failing to employ reasonable measures to secure the Private Information at issue.

185. This Court should also issue corresponding prospective injunctive relief requiring HUB to employ adequate security protocols consistent with legal and industry standards to protect Plaintiff's and Class Members' Private Information, including the following:

a. Order HUB to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, HUB must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on HUB's systems on a periodic basis, and ordering HUB to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of HUB's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating Plaintiffs and Class Members about the threats they face with regard to the security of their Private Information, as well as the steps victims of the HUB Data Breach should take to protect themselves.

186. If an injunction is not issued, Plaintiff will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at HUB. The risk of another such breach is real, immediate, and substantial. If another breach at HUB occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

187. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to HUB if an injunction is issued. Plaintiff will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of HUB's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and HUB has a pre-existing legal obligation to employ such measures.

188. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at HUB, thus preventing future injury to Plaintiff and Class Members whose Private Information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Classes described above, seeks the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class and requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing HUB to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring HUB to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: August 28, 2023.

Respectfully submitted,

/s/ Mason A. Barney

Mason A. Barney, Bar No. 4405809
Tyler J. Bean (*pro hac vice* application forthcoming)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: mbarney@sirillp.com
E: tbean@sirillp.com